UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

1) SURGICAL PARTNERS OF OKLAHOMA, PLLC, 2) Individually and on behalf of all others similarly situated, Plaintiff, v. 1) CHANGE HEALTHCARE, INC., 2) OPTUM, INC., and 3) UNITEDHEALTH GROUP INCORPORATED Defendants.	**Case No. CIV-24-625-D** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Surgical Partners of Oklahoma, PLLC ("Plaintiff"), brings this class action complaint against Defendants, Change Healthcare Inc. ("Change"), Optum, Inc. ("Optum"), and UnitedHealth Group Incorporated ("UHG") and alleges the following:

INTRODUCTION

1. Plaintiff and putative class members' business operations have been harmed by Defendants' negligence in securing and safeguarding their information systems from a foreseeable cyberattack.

2. Change is a part of Optum, which in turn is part of the healthcare conglomerate, UHG. Optum completed its merger with the software and data analytics firm, Change, in 2021, after a challenge of the deal by the Department of Justice for being anticompetitive was rejected by a Washington DC federal judge.

3. Change manages health care technology pipelines, processing 14 billion transactions a year. It offers a range of services to the healthcare sector, including payment and billing, prescription processing and data analytics. connecting approximately 900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories. Medical records of one in every three American patients passes through Change's digital systems. It processes $1.5 trillion in medical claims annually. The company reported $920 million in total revenue for the 2022 fiscal year.

4. On February 12, 2024, cybercriminals took advantage of weaknesses in Change's cybersecurity processes to access its network.

5. Change first reported the network outage on February 21, 2024, and later said the problem was a "cybersecurity issue" from an outside threat.

6. It was only on February 29, 2024, after the Russian-speaking ransomware group AlphV, also known as Blackcat ("Blackcat"), in a since deleted message on the dark web, claimed responsibility for the attack that Change confirmed that its systems had been penetrated by the group.

7. Blackcat, a well-known cybergroup, breaches healthcare institutions by exploiting network vulnerabilities, using ransomware to attack valuable targets. They then demand payment for decryption keys, but even when paid, they may still leak data onto the Dark Web. Blackcat ranks as one of the top ransomware service providers globally.

8. The attack resulted in severe network interruptions and the seizure of 6 terabytes of crucial, confidential information, affecting millions of patients and physicians.

Blackcat claimed that it exfiltrated data that "relates to all Change Health clients that have sensitive data being processed by the company."[1]

9. According to publicly reported information, the Data Breach involved a ransomware attack, wherein the cybercriminals accessed Change Healthcare's systems and encrypted Change's data to hold it hostage in seeking a ransom payment. It was reported that Change paid Blackcat a ransom of 350 bitcoins, or approximately $22 million.

10. Change handles and stores sensitive patient data that range from phone numbers, addresses, Social Security numbers to medical, dental, and insurance records for millions of individuals. Blackcat accessed and copied vast amounts of this data.

11. Furthermore, being a subsidiary of a major healthcare insurer, UHG, Change processes a massive number of transactions annually, affecting a significant portion of U.S. patient records. The data breach has severely impacted the healthcare sector and will continue to do so.

12. In response to the attack, Change disconnected its affected systems, hamstringing providers and disrupting key operations such as pharmacy orders, as providers have not been able to communicate pharmacy prescriptions and pharmacies have been unable to verify patient eligibility and coverage. As a result, patients with life threatening diseases have been facing difficulty accessing essential medications.

[1] *See* https://healthitsecurity.com/news/change-healthcare-disconnects-system-amid-cyberattack#:~:text=2%2F29%2F2024%20%2D%20Change,latest%20notice%20to%20customers%20stated (last accessed on June 6, 2024).

13. However, the repercussions of the data breach extend beyond patients to healthcare providers like the Plaintiff, whose operations rely on Change's services for claims processing.

14. Healthcare providers are still grappling with the aftermath of the data breach, facing financial strain and potential closure. They have been unable to file claims and receive normal cash flow to support operations. As a result, they have been forced to incur additional expenses by transitioning to alternative claim processing platforms. Small and mid-sized practices are harmed the most, as they continue to treat patients, adjust to a new system, and pay for another service, all while they are weeks behind on receiving payment. These less resourced provider services cannot tolerate a months-long disruption of their cash reserves, and such disruption causes an existential threat to these providers.

15. While healthcare providers are dealing with severe revenue interruption as a result of Change's negligence, Change continues to charge subscribers, adding insult to injury for healthcare providers already struggling with the fallout of the breach.

16. Change neglected to implement adequate security measures. The system weakness exploited by Blackcat hackers was easily identifiable and curable. Change's failure to take the required steps to prevent the attack resulted in significant financial losses and operational disruptions for healthcare providers.

17. The consequences of Change's actions have been dire for many healthcare providers, with some facing the possibility of insolvency and others having to resort to extreme measures to maintain operations.

18. As a direct and proximate result of Change's failures, Plaintiff and the Class Members have suffered serious injury.

19. Accordingly, Plaintiff, on behalf of itself and similarly situated healthcare providers who were harmed by the data breach and ransomware attack, seeks to hold Defendant responsible for harms caused by Defendant's negligence.

PARTIES

20. Plaintiff Surgical Partners of Oklahoma, PLLC is a professional service company organized in the State of Oklahoma, with a principal place of business located in Edmond, Oklahoma.

21. Defendant Change Healthcare Inc. is a Delaware corporation with its principal place of business in Nashville, Tennessee.

22. Defendant Optum, Inc. is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota.

23. Defendant UnitedHealth Group is among the largest publicly traded companies by revenue and is a Delaware corporation with its principal place of business in Minnetonka, Minnesota. UnitedHealth Group oversees the management of Change Healthcare's cybersecurity systems, as demonstrated by their response to the data breach detailed herein.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members

and at least some members of the proposed Class have a different citizenship from Change and other Defendants. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

25. This Court has personal jurisdiction over Defendants because they are authorized to and conduct business in this District.

26. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b)(1) & (2) because a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

27. Change is a healthcare services and support company that provides revenue and payment cycle management to healthcare providers. It connects payers, providers, and patients within the US healthcare system. Change is the predominant source of more than 100 critical functions that keep the US healthcare system operating. Among these functions, Change manages the clinical criteria used to authorize a substantial portion of patient care and coverage, processes billions of claims, supports clinical information exchange, and processes drug prescriptions. The company promotes itself as offering "data and analytics, plus patient engagement and collaboration tools" to help "providers, payers, third-party administrators, and pharmacies". Change Healthcare is a major player in

processing prescription medications in the United States and manages billing for pharmacies nationwide, handling "15 billion healthcare transactions each year."[2]

28. Change specializes in "moving patient data from doctor's office, or to and from your insurance company." This includes Social Security numbers, medical records, insurance information, and more.[3]

29. Given the volume and sensitive nature of the data it stores, Change has a privacy policy that outlines how confidential and personal information is used and disclosed. The policy states: "We implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse. These measures are aimed at providing ongoing integrity and confidentiality of data, including your personal information."

30. Change's prior statements about data security demonstrate that it was fully aware of its responsibility to protect patients' Personal Health Information (PHI) and Personal Identifiable Information (PII).

The Data Breach

31. On February 21, 2024, UHG reported in its required 8-K SEC filing that "a suspected nation-state associated cybersecurity threat actor had gained access to some of

[2] Ron Wyden, Wyden Hearing Statement on Change Healthcare Cyberattack and UnitedHealth Group's Response (May 1, 2024), .https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf.gov/imo/media/doc/0501_wyden_statement.pdf (last visited June 12, 2024)

[3] *Id*.

the Change Healthcare information technology systems."[4] After detecting the breach, UHG claimed to have "proactively isolated the impacted systems from other connecting systems."[5] UHG also stated it was "working with law enforcement" and had "notified customers, clients, and certain government agencies" about the breach.[6] UHG clarified that the "network interruption [was] specific to Change Healthcare."[7]

32. According to the cybercriminal group responsible for the attack, Blackcat, the stolen data included millions of records, such as active US military/navy personnel PII, medical records, payment information, claims information, patients' PII including phone numbers, addresses, Social Security number, email addresses, insurance records, among others.

33. Healthcare providers, who have paid for Change's services, use the platform to submit insurance claims. Change then forwards these claims to health insurance companies for evaluation and processing. Subsequently, providers receive reimbursement payments from the insurance companies.

34. Following the Data Breach, Change disconnected its platform. The Change Platform was inoperable from the time of the breach and was expected to remain down until at least mid-March. On March 18, 2024, Change informed customers that they could expect to be reconnected by the week of March 25, 2024.

---

[4] UnitedHealth Group Incorporation Form 8-K, SEC (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm

[5] *Id.*

[6] *Id.*

[7] *Id.*

35. Since the Change Platform handles 15 billion healthcare transactions annually, affecting about one in three U.S. patient records, its outage disrupted a vast number of healthcare providers' claims. For many providers who rely solely on Change for claim processing, their payments were entirely halted during the outage.

36. The potential impact of the Data Breach is staggering while its effects are currently being felt by healthcare providers and payers nationwide.

The Data Breach and Resulting Shutdown were Foreseeable Risks of Which Defendants were on Notice and Could Have Prevented.

37. Cybercriminals target the healthcare industry the most due to the treasure trove of confidential health and personal information maintained and stored by healthcare organizations.

38. Cyberattacks have doubled from 2016 to 2021 and have resulted in the exposure of personal health information for approximately 42 million patients.[8]

39. The most prevalent and successful method of illicitly accessing a company's internal networks has historically been through the use of stolen credentials. It's imperative for companies to implement proactive measures to prevent such attacks.

40. As early as 2014, the FBI warned healthcare stakeholders that they are the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare

[8] *See* https://www.npr.org/sections/health-shots/2024/03/09/1237038928/health-industry-ransomware-cyberattack-change-healthcare-optum-uhc-united (last accessed on June 12, 2024).

related systems perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).”[9]

41. On October 28, 2020, the FBI and two federal agencies released a "Joint Cybersecurity Advisory" alerting to "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[10] The advisory, issued by the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (“HHS”), and the FBI, urged healthcare providers to promptly implement "timely and reasonable precautions" to safeguard their networks against these threats.[11]

42. In 2023, the FBI reported 249 ransomware attacks in the healthcare industry.

43. According to the HHS, Office for Civil Rights, the health care sector has been experiencing a 278% increase in large breaches involving ransomware which has led to “extended care disruptions, patient diversions to other facilities, and delayed medical procedures, all putting patient safety at risk.”[12]

---

[9] *See* https://publicintelligence.net/fbi-targeting-healthcare20(PII) (last accessed on May 17, 2024).)

[10] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last accessed June 12, 2024).

[11] *Id*.

[12] HHS Press Office, “HHS Announces Next Steps in Ongoing Work to Enhance Cybersecurity for Health Care and Public Health Sectors” https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html (last accessed June 12, 2024)

44. Approximately 80% of ransomware is delivered through email phishing attacks.[13] Other means to deliver ransomware is through brute force attacks on open remote desktop protocol ports.

45. The primary methods for reducing the risk of stolen credentials are through user education and the implementation of technical security measures.

46. To prevent ransomware attacks, organizations must provide training to its employees for the handling of suspicious emails. They can also disable macros, avoid storing passwords in plain text, and perform hunts and search for suspicious behavior in their networks, among other things.

47. This is not the first time that the UHG family has dealt with a data breach. In May 2023, United HealthCare, a UHG subsidiary, had to notify members that protective health information may have been compromised due to a credential stuffing attack that occurred on the United Healthcare mobile app in February 2023.

48. Accordingly, Defendants knew that given the vast amount of PHI and PII that healthcare providers such as Plaintiff and Class members acquire and transmit to Defendants directly or through vendors, and that in turn, Defendants store and maintain, they were a target for cybercriminals and should have taken all reasonable measures to avoid cyberattacks.

[13] https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/#:~:text=In%202020%2C%20phishing%20was%20responsible,99%20contains%20a%20phishing%20attack. (last accessed June 12, 2024).

49. Defendants also understood the risks posed by their insecure data security practices and computer networks. Defendants' failure to heed warnings and failure to adequately maintain their computer networks secure resulted in the shutdown and harm to Plaintiff and Class members.

50. Despite their crucial position in the healthcare sector, Defendants neglected to adhere to the recommended best practices outlined by CISA. Had Defendants implemented basic security measures, the hackers would have been unable to access millions of patient files, potentially preventing the breach entirely or significantly limiting its scope. Additionally, Change lacked essential safeguards to prevent and detect phishing attacks and failed to establish sufficient monitoring or control systems to identify unauthorized infiltration post-breach.

51. Defendants' failure to adhere to industry standards is unjustifiable, particularly considering their awareness of being a prime target for cyberattacks.

52. Defendants knew that a breach of their computer system, and exposure of the information stored therein, would very likely necessitate taking their systems offline to address the resulting issues, thereby depriving healthcare providers of critical services. Accordingly, Defendants had a duty to implement a backup system that would fulfill the basic functions for Plaintiffs and members of the proposed Class in the event of a cybersecurity incident such as the February 2024 data breach.

The Aftermath of the Data Breach

53. Following the Data Breach, Change shut down a significant portion of its network, including its Change Platform, which is utilized by healthcare providers across the country for payment and treatment purposes. However, Change made this decision without offering a sufficient alternative, leading to widespread devastation among healthcare practices nationwide.

54. With the disconnection of the Change Platform, numerous healthcare providers have lost their primary, and in some instances, sole means of processing payments for their services through patients' healthcare plans, resulting in a lack of payment. Consequently, healthcare providers are bearing the brunt of these upfront costs.

55. With dwindling account balances and outstanding reimbursements, many healthcare providers find themselves in precarious financial situations. For instance, Arlington Urgent Care, a chain of five urgent care centers in Columbus, Ohio, is grappling with approximately $650,000 in unpaid insurance reimbursements. To cover essential expenses like employee payroll and rent, the owners have resorted to securing lines of credit from banks and dipping into their personal savings.[14] Meanwhile, other healthcare providers are facing challenges such as duplicated payment software charges. Florida Cancer Specialists and Research Institute in Gainesville, for instance, switched to two other healthcare software platforms, as they spend a substantial amount—$300 million

[14] Reed Abelson & Julie Creswell, *Cyberattack Paralyzes the Largest U.S. Healthcare Payment System*, NYTIMES (Mar. 7, 2024), https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html (last accessed June 12, 2024)

monthly—on chemotherapy and other critical medications that cannot be delayed for patients' treatments.[15] Additionally, some healthcare providers are forced to make difficult decisions, such as reducing resources for patients, to navigate through these challenging times. A Philadelphia-based primary care practice with 20 clinicians, for example, has been mailing off "hundreds and hundreds" of pages of Medicare claims and is considering trimming expenses by reducing the supply of vaccines available at the clinic.[16]

56. Healthcare providers have paid for Change's services that they are currently not receiving. Without access to these services, providers and practices are facing difficulties in delivering patient care and experiencing financial losses.

Defendants Failed to Comply with Federal Law and Regulatory Guidance.

57. By obtaining, collecting, using, and deriving a benefit from PHI and PII, Defendants assumed the duty of protecting such information from unauthorized disclosure. In addition to their common law duties, Defendants' duty to use reasonable security measures arose, in part, under Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as outlined in 45 C.F.R. § 160.102. On its website Change states that it "functions as a HIPAA business associate for its HIPAA covered entity payer and provider customers as its primary business function," so Change is admittedly subject to HIPAA regulations.

[15] *Id.*
[16] *Id.*

58. As a business covered under HIPAA, Change is required to comply with HIPAA rules, including the Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (which establish standards for the privacy of individually identifiable health information), and the Security Rule (which specify security standards for the protection of electronic protected health information), 45 C.F.R. Part 160 and Part 164, Subparts A and C. HIPAA requires, *inter alia*, that Change reasonably protect PHI from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

59. HIPAA restricts the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information." 45 C.F.R. § 164.502.

60. HIPAA mandates that Change implement suitable safeguards for this information. 45 C.F.R. § 164.530(c)(1).

61. HIPAA mandates that Change notifies individuals in the event of a breach of unsecured protected health information. This includes protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals, such as non-encrypted data. 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

62. Despite these obligations, Defendants failed to fulfill their duties under HIPAA. Specifically, *inter alia*, Change failed to: (1) Ensure the maintenance of a sufficient data security system to mitigate the risk of data breaches and cyberattacks; (2) Enact technical policies and procedures for electronic information systems that handle electronically protected health information; (3) Implement adequate policies and

procedures to prevent, detect, contain, and correct security violations; (4) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations; (5) Adequately protect the confidentiality and integrity of electronically stored or transmitted PHI.

63. Moreover, businesses entrusted with sensitive data have been furnished with authoritative and readily accessible resources aimed at mitigating the risks of cyberattacks. For instance, the Federal Trade Commission ("FTC") has released several guides for businesses underscoring the significance of employing reasonable data security practices, which should inform all decision-making processes related to business operations.[17]

64. Among other recommendations, the guidelines advise that businesses should safeguard the personal customer information they collect and store, properly dispose of personal information that is no longer needed, encrypt information stored on their computer networks, understand vulnerabilities within their network, and implement policies to address security issues. Additionally, the FTC guidelines suggest that businesses utilize an intrusion detection system, monitor incoming traffic for any unusual activity, watch for large volumes of data being transmitted from their system, and have a response plan prepared in the event of a breach.[18]

---

[17] *Start with Security*, FTC, https://www.ftc.gov/system/files/documents/plainlanguage/pdf0205-startwithsecurity.pdf (last visited June 12, 2024).

[18] *Id*.

65. Additionally, the FTC recommends that companies restrict access to sensitive data, mandate the use of complex passwords for network access, employ industry-tested security methods, monitor networks for any suspicious activity, and ensure that third-party service providers have implemented reasonable security measures.[19] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA 2020 guidance.

66. Businesses that neglect to adequately protect customer information have faced FTC enforcement actions. The FTC regards the failure to implement reasonable and appropriate measures to safeguard against unauthorized access to confidential consumer data as an unfair act or practice, which is prohibited by Section 5 of the Federal Trade Commission Act. 15 U.S.C. § 45. Orders resulting from these actions provide additional clarity on the steps businesses must take to fulfill their data security obligations.[20]

67. Despite being fully cognizant of its obligation to protect patients' PHI, Change neglected to adhere to fundamental recommendations and guidelines that could have averted this breach. Moreover, despite awareness of prior cyberattacks, Change failed to take adequate measures. Change's failure to implement reasonable cybersecurity measures to prevent unauthorized access to patient information constitutes an unfair act or practice, which is proscribed by the FTC Act. 15 U.S.C. § 45.

---

[19] *Start With Security*, supra note 32.

[20] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/newsevents/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited June 12, 2024).

Allegations Relating to Plaintiff

68. Plaintiff is an Oklahoma healthcare provider with an office in Yukon, Oklahoma.

69. Plaintiff has contracted with services that use the Change Platform to submit bills/reimbursement forms on behalf of their clients like Plaintiff.

70. About the middle to late February, Plaintiff became aware that its reimbursement claims were not being processed and it was not receiving payments for services it had provided.

71. Upon information and belief, Change had disconnected its systems.

72. Once the Data Breach occurred and Change disabled its Platform, Plaintiff was unable to submit reimbursement requests/bills for its patients.

73. Upon information and belief, the disruption of processing and payment of Plaintiff's bills is the result of Change's decision to disconnect the network after the Data Breach. This disconnection was reasonably foreseeable to Change due to the failure to protect its network from cyberattacks.

74. Plaintiff continued to treat patients during the Change outage, without any certainty about when payment would be received.

75. Currently, Plaintiff estimates losses in excess of $75,000 based on outstanding medical bills that were not processed due to the Change outage.

76. Due to the inability to submit bills and get paid for services rendered to its patients after the Change Platform was disabled, Plaintiff experienced a backlog of unpaid revenues, which has impacted their ability to operate and treat their patients.

CLASS ACTION ALLEGATIONS

77. Plaintiff seeks relief in their individual capacity and as representatives of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23, Plaintiff brings their action on behalf of themselves, and the Nationwide Class defined as:

> All healthcare providers whose reimbursement payments were delayed following the Data Breach announced by Change, Optum, and/or UnitedHealth Group Inc. in February 2024.

78. Plaintiff reserves the right to re-define the Class definitions after conducting discovery.

79. Specifically excluded from the Class are Defendants; their officers, directors, or employees; any entity in which Defendants have a controlling interest; and any affiliate, legal representative, heir, or assignees of Defendants.

80. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

81. The proposed Class meets all the requirements of the Federal Rules of Civil Procedure 23(b) as set forth below:

82. **Class Identity**: The members of the Class are readily identifiable and ascertainable. Change and/or its affiliates, among others, possess the information to identify and contact class members.

83. **Numerosity**: The members of the Class are so numerous that joinder of all of them is impracticable. According to the U.S. Department of Health and Human Services, Change "processes 15 billion health care transactions annually and is involved in one in

every three patient records." According to Change, it is connected to "more than 600,000 providers[.]"

84. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class because all class members reimbursement payments were delayed following the Data Breach and were harmed as a result.

85. **Adequacy**: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no known interest antagonistic to those of the Class and its interests are aligned with Class members' interests. Plaintiff's reimbursement payments were delayed following the Data Breach just as class members, and suffered similar harms. Plaintiff has also retained competent counsel with significant experience litigating complex and commercial class actions.

86. **Commonality and Predominance**: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

- Whether Change owed Plaintiff and Class members a duty to implement and maintain reasonable security procedures and practices to protect patients' PHI;
- Whether Change acted negligently in connection with the monitoring and/or protection of Plaintiff and Class members' PHI;
- Whether Change violated its duty to implement reasonable security systems to protect Plaintiff and Class members' PHI;
- Whether Change's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and Class members;

- Whether Change adequately addressed and fixed the vulnerabilities that enabled the Data Breach;
- Whether Class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

87. Defendants have engaged in a common course of conduct and Plaintiff and Class members have been similarly impacted by their failure to maintain reasonable security procedures and practices to protect patients' PHI.

88. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CAUSES OF ACTION
COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

89. Plaintiff repeats and reallege every allegation set forth in the preceding paragraphs.

90. Defendants required patients' PHI as a prerequisite of receiving healthcare services and to perform their functions in connection with patients receiving medical treatment. Defendants stored the data for the purposes of providing health insurance services as well as for commercial gain.

91. Defendants owed Plaintiff and class members a duty to exercise reasonable care in protecting patients' PHI from unauthorized disclosure or access. Change acknowledged this duty in its privacy policies, where it promised not to disclose PHI, including SSNs, without authorization and to abide by all federal laws and regulations.

92. Defendants owed a duty of care to Plaintiff and class members to provide adequate data security, consistent with industry standards, to ensure that Change's systems and networks adequately protected the PHI.

93. Defendants' duty to use reasonable care in protecting PHI arises from common law and federal law, including the HIPAA regulations described above and Change's own policies and promises regarding privacy and data security.

94. Defendants knew, or should have known, of the risks inherent in collecting and storing PHI in a centralized location, Change's vulnerability to network attacks, and the importance of adequate security.

95. Plaintiff and class members were foreseeable and probable victims of any inadequate cybersecurity practices.

96. Defendants breached their duty to Plaintiff and class members in numerous ways, as described herein, including by:

- Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect patients' PHI;
- Failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;
- Failing to comply with its own privacy policies;
- Failing to comply with regulations protecting the PHI at issue during the period of the Data Breach; and
- Failing to adequately monitor, evaluate, and ensure the security of Change's network and systems.

97. Patients' PHI would not have been compromised but for Defendants' wrongful and negligent breach of its duties.

98. Change would not have disconnected the Change Platform but for its wrongful and negligent breach of their duties.

99. Given that healthcare providers and affiliates are prime targets for hackers, Defendants' failure to take proper security measures to protect patients' PHI, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and copying of PHI by unauthorized third parties. It was also foreseeable that as a result of a data breach, Change would have to disconnect systems that could disrupt healthcare practices.

100. As a direct and proximate result of Defendants' conduct, Plaintiff and class members have suffered damages, including missed payments and out-of-pocket expenses

associated with (i) purchasing new healthcare payment software; (ii) notifying patients of data breach; and (iii) late penalties assessed for untimely payment of expenses. Furthermore, Plaintiff and class members' damages include time and effort spent researching and implementing new healthcare payment software.

COUNT TWO
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Class)

101. Plaintiff restates and re-alleges every allegation of the preceding paragraphs of this Complaint.

102. Defendants entered into contracts with Plaintiff.

103. Defendants agreed to provide their specialized services in a professional and workmanlike manner. Implicit in performing these contractual duties is an obligation to reasonably safeguard their systems and data from cyberattack, including ransomware attacks, which can cause an interruption in the flow of an enterprise's routine and everyday services to its clients.

104. Defendants breached their contracts with the Plaintiff and Entity Subclass members by failing to reasonably safeguard their systems and data from cyberattack, including ransomware attacks.

105. As a direct and proximate result of Defendants' contract breaches, Plaintiff and the Entity Subclass sustained actual losses and damages including, but not limited to, complete interruption and disruption of its ability to obtain reimbursement services provided to their patients or clients.

COUNT THREE
UNJURST ENRICHMENT
(On Behalf of Plaintiff and the Class)

106. Plaintiff restates and re-alleges every allegation of the preceding paragraphs of this Complaint.

107. Plaintiff and Class members conferred benefits on the Defendants in the form of payment for claims management and processing, insurance verification, authorization and medical necessity reviews, and disbursement of payments, among other things, both directly and indirectly. Defendants had knowledge of the benefits conferred by Plaintiff and Class members and appreciated such benefits. Defendants should have used, in part, the monies Plaintiff and Class members paid to them, directly and indirectly, to pay the costs of reasonable data privacy and security procedures.

108. Defendants state that they devote "significant resources" to protect PHI, a portion of which is derived from the benefit conferred by the contractual payments made by Plaintiff and Class members to Defendant.

109. Plaintiff and Class members have suffered actual damages and harm as a result of the Defendant's conduct, inactions, and omissions. Defendants should be required to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received from Plaintiff and Class members.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

a. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representatives and Plaintiff's counsel as Class Counsel;

b. That the Court award Plaintiff and class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

c. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

d. That Plaintiff be granted the declaratory relief sought herein;

e. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

f. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: June 17, 2024

Respectfully submitted,

/s/ *Matthew J. Sill*
MATTHEW J. SILL (OBA 21547)
TARA TABATABAIE (OBA 21838)
SILL LAW GROUP, PLLC
1101 N. Broadway Ave., Suite 102
Oklahoma City, OK 73103
Tel: (405) 509-6300
Fax: (800) 978-1345
Counsel for Plaintiff & the Putative Class